Available online at www.sciencedirect.com
ScienceDirect
Journal of Pure and Applied Algebra 212 (2008) 910–918
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

The structure of algebras admitting well-agreeing near weights

Carlos Munuera[a,*], Fernando Torres[b]

[a] *Department of Applied Mathematics, University of Valladolid, Avda Salamanca SN, 47014 Valladolid, Castilla, Spain*
[b] *IMECC-UNICAMP, Cx.P. 6065, 13083-970, Campinas, SP, Brazil*

Received 20 February 2007; received in revised form 25 May 2007; accepted 11 July 2007
Available online 5 September 2007

Communicated by J. Walker

Abstract

We characterize algebras admitting two well-agreeing near weights. These algebras can be used for constructing error-correcting codes of algebraic geometric type over two points, by using elementary methods only.

MSC: 94B27; 13A18

1. Introduction

Algebraic geometric codes (or AG codes, for short) were constructed by Goppa [6,7], based on a curve $\mathcal{X}$ over a finite field $\mathbb{F}$ and two rational divisors D and G on $\mathcal{X}$, where D is a sum of pairwise distinct points and $G = \alpha_1 P_1 + \cdots + \alpha_m P_m$, with $P_i \notin \operatorname{supp}(D)$. Soon after its introduction, AG codes became a very important tool in Coding Theory; for example, Tsfasman, Vladut and Zink [17] showed that the Varshamov–Gilbert bound can be attained by using these codes. However, the study of AG codes relies on the use of algebraic geometric tools, which is difficult for nonspecialists in algebraic geometry. In 1998, Høholdt, van Lint and Pellikaan presented a construction of AG codes 'without algebraic geometry', that is, by using elementary methods only [8] (see also [4]). These methods include order and weight functions over an $\mathbb{F}$-algebra and semigroup theory mainly. From that paper, order domains and order functions and the corresponding obtained codes have been studied by many authors; to mention a few of them: Pellikaan [15], Geil and Pellikaan [5] and Matsumoto [11].

The approach given by Høholdt, van Lint and Pellikaan allows us to work with the so-called 'one-point' AG codes, that is when the divisor G is a multiple of a single point, $G = \alpha P$. A generalization of the same idea to 'two-point' AG codes ($m = 2$) was given in [1]. To that end, variations of order and weight functions over an $\mathbb{F}$-algebra R—the so-called *near order* and *near weight* functions—were introduced in that paper. By using these results we can manage AG codes in terms of algebras, near weights and semigroups. This is possible whenever such near weights verify a technical condition of well-agreement (see Section 2 for an explanation of these concepts). On the other hand,

* Corresponding author. Fax: +34 983 423451.
E-mail addresses: cmunuera@modulor.arq.uva.es (C. Munuera), ftorres@ime.unicamp.br (F. Torres).

0022-4049/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2007.07.006

to construct codes by using these ideas, it is crucial to characterize the algebras admitting those well-agreeing near weights. This task is accomplished in this paper.

We shall characterize algebras R admitting two well-agreeing near weights ρ and σ, as being certain subalgebras of the regular function ring of an affine variety of type $\mathcal{X} \setminus \{P, Q\}$, where $\mathcal{X}$ is a projective, geometrically irreducible, nonsingular algebraic curve and P and Q are two different points of $\mathcal{X}$. We will also show that ρ and σ are defined by the valuations at P and Q respectively (see Theorem 5.6 in Section 5). This result is essentially analogous to the characterization of algebras admitting a weight function given by Matsumoto [11].

For simplicity, throughout this work we shall use the language in terms of algebraic function fields instead of algebraic curves.

2. Preliminaries: Orders, n-orders and codes

In order to provide a framework for our results and for the convenience of the reader, we begin by recalling some facts about orders and near orders as well as their uses for constructing codes.

2.1. Order functions

Our reference here is the article [8]. Let $\mathbb{N}_0$ be the set of nonnegative integers and $\mathbb{F}$ a finite field. Throughout this paper, by an $\mathbb{F}$-algebra we mean a commutative $\mathbb{F}$-algebra with identity, R, such that $\mathbb{F} \subsetneq R$. Given the $\mathbb{F}$-algebra R, a function $\rho : R \to \mathbb{N}_0 \cup \{-\infty\}$ is called an *order* function on R if for all $f, g, h \in R$, the following properties are satisfied:

(O0) $\rho(f) = -\infty$ if and only if $f = 0$;
(O1) $\rho(\lambda f) = \rho(f)$ for all $\lambda \in \mathbb{F}^*$;
(O2) $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$;
(O3) If $\rho(f) < \rho(g)$ and $h \neq 0$, then $\rho(fh) < \rho(gh)$; and
(O4) If $\rho(f) = \rho(g) \neq -\infty$, then there exists $\lambda \in \mathbb{F}^*$ such that $\rho(f - \lambda g) < \rho(g)$.

If in addition

(O5) $\rho(fg) = \rho(f) + \rho(g)$,

then ρ is called a *weight* function. As was said before, order and weight functions were introduced and used by Høholdt, van Lint and Pellikaan to construct codes of AG type by using elementary methods only (that is, without algebraic geometry). This construction works as follows: take an $\mathbb{F}$-algebra R admitting an order function ρ. Then there exists a basis $\{f_i : i \in \mathbb{N}\}$ of R over $\mathbb{F}$ such that $\rho(f_i) < \rho(f_{i+1})$ for all i. Let L_ℓ be the vector space spanned by $f_1, \ldots, f_\ell$, and let $\phi : R \to \mathbb{F}^n$ be a surjective morphism of $\mathbb{F}$-algebras. The obtained codes are $E_\ell = \phi(L_\ell)$ and its dual $C_\ell = E_\ell^\perp$. The minimum distance of C_ℓ can be bounded by the so-called *order bound*. When ρ is a weight the order bound only depends on the semigroup $H(R) = \{\rho(f) : f \in R^*\}$. In this case, it is often known as the *Feng–Rao bound*.

2.2. Characterizing $\mathbb{F}$-algebras admitting weight functions

To apply the above results and obtain the corresponding codes, it is necessary to characterize the $\mathbb{F}$-algebras admitting weight functions. For example, it is shown in [8] that they are always integral domains. The full characterization of such algebras was given by Matsumoto [11], as follows: let R be an $\mathbb{F}$-algebra admitting a weight function ρ. Then there exists a nonsingular, algebraically irreducible, projective algebraic curve $\mathcal{X}$ and a point $P \in \mathcal{X}$ such that

- the integral closure of R in its quotient field is the ring of regular functions of the affine curve $\mathcal{X} \setminus \{P\}$;
- $\rho = -v_P$, where v_P is the valuation at P.

2.3. N-order functions

As was said in the introduction, the above construction allows us to work with one-point AG codes. The generalization to multiple-point AG codes was given by Carvalho, Munuera, Silva and Torres in [1]. The first step of this generalization is to change a little bit the kind of orders we have to manage.

For a function $\rho : R \to \mathbb{N}_0 \cup \{-\infty\}$, let us consider the sets

$$\mathcal{U}^* = \mathcal{U}^*_\rho := \{r \in R \setminus \{0\} : \rho(r) \leq \rho(1)\};$$
$$\mathcal{M} = \mathcal{M}_\rho := \{r \in R : \rho(r) > \rho(1)\}$$

and $\mathcal{U} = \mathcal{U}_\rho := \mathcal{U}^* \cup \{0\}$. The function ρ is called a *near weight* (or an *n-weight*, for short) if the following conditions are satisfied. For all $f, g, h \in R$ and $\lambda \in \mathbb{F}^* := \mathbb{F} \setminus \{0\}$:

(N0) $\rho(f) = -\infty$ if and only if $f = 0$;
(N1) $\rho(\lambda f) = \rho(f)$;
(N2) $\rho(f + g) \leq \rho(f) + \rho(g)$;
(N3) If $\rho(f) < \rho(g)$, then $\rho(fh) \leq \rho(gh)$. Furthermore, if $h \in \mathcal{M}$ then $\rho(fh) < \rho(gh)$;
(N4) If $\rho(f) = \rho(g)$ with $f, g \in \mathcal{M}$, then there exists $\mu \in \mathbb{F}^*$ such that $\rho(f - \mu g) < \rho(f)$;
(N5) $\rho(fg) \leq \rho(f) + \rho(g)$ and equality holds if $f, g \in \mathcal{M}$.

An n-weight becomes a *weight function*, as defined in Høholdt, van Lint and Pellikaan if and only if $\mathcal{U} = \mathbb{F}$ [1, Lemma 3.3].

If ρ is an n-weight, then so is $d\rho$ for all $d \in \mathbb{N}$. Then we define the *normalization* of ρ as the n-weight $\tilde{\rho}$ given by $\tilde{\rho}(f) = 0$ for $f \in \mathcal{U}^*$ and $\tilde{\rho}(f) = \rho(f)/d$ for $f \in \mathcal{M}$, where $d = \gcd\{\rho(f) : f \in \mathcal{M}\}$ (see [1, Sect. 3.2]). In what follows in this paper, all the n-weights will be *normal*, that is $\rho = \tilde{\rho}$. For given two (normal) n-weights ρ and σ over the $\mathbb{F}$-algebra R, set

$$H = H(R) := \{(\rho(f), \sigma(f)) : f \in R^*\},$$

where $R^* = R \setminus \{0\}$. We say that ρ and σ *agree well* if $\#(\mathbb{N}_0^2 \setminus H)$ is finite and $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$. In the next section we will prove that H is a semigroup so that this definition will in fact be compatible with the one given in [1]. Algebras admitting well-agreeing n-weights exist, as the next example shows.

Example 2.1. Let $\mathbf{K}$ be an algebraic function field of one variable over $\mathbb{F}$, such that $\mathbb{F}$ is the full constant field of $\mathbf{K}$. For a place S of $\mathbf{K}$, let $\mathcal{O}_S$ be the local ring at S and v_S its corresponding valuation. Let P, Q be two different places of $\mathbf{K}$. Consider an $\mathbb{F}$-algebra $R \subseteq \mathbf{K}$ and define

$$\varrho'(f) := \begin{cases} -\infty & \text{if } f = 0, \\ 0 & \text{if } v_P(f) \geq 0, \\ -v_P(f) & \text{if } v_P(f) < 0 \end{cases} \qquad \varsigma'(f) := \begin{cases} -\infty & \text{if } f = 0, \\ 0 & \text{if } v_Q(f) \geq 0, \\ -v_Q(f) & \text{if } v_Q(f) < 0. \end{cases}$$

Let ϱ and ς be the normalization of ϱ' and ς' respectively. If $R = R(P, Q) := \bigcap_{S \neq P,Q} \mathcal{O}_S$, then ϱ and ς are well-agreeing n-weights over R.

Remark 2.2. The normalization process could be crucial in order to have well-agreeing n-weights, as the following example shows. Let $\mathbf{K} := \mathbb{F}_2(x)$ be the rational function field of characteristic two. Let S be the ring of all functions of $\mathbf{K}$ which are regular away from two places P, Q, and let $R := \{f^2 : f \in S\}$. Let ϱ', ς' and ϱ, ς, be the n-weights obtained from P and Q by using the procedure stated in Example 2.1, before and after normalization. Then clearly $\mathcal{U}_{\varrho'} \cap \mathcal{U}_{\varsigma'} = \mathcal{U}_\varrho \cap \mathcal{U}_\varsigma = \mathbb{F}$, but when considering ϱ', ς', we have that $\#(\mathbb{N}_0^2 \setminus H(R))$ is infinite (as all points in $H(R)$ have even coordinates), whereas when considering ϱ, ς, we have that $\#(\mathbb{N}_0^2 \setminus H(R)) = \#(\mathbb{N}_0^2 \setminus H(S))$ is finite.

We state a property of n-weights that we shall need later.

Lemma 2.3. *Let $f \in R^*$ and $g \in \mathcal{U}_\rho \setminus \mathbb{F}$. Then there exists $\lambda \in \mathbb{F}$ such that $\rho(f(g - \lambda)) < \rho(f)$.*

Proof. According to (N5), $\rho(fg) \leq \rho(f)$. If $\rho(fg) = \rho(f)$, by (N4) there exists $\lambda \in \mathbb{F}$ such that $\rho(f(g-\lambda)) = \rho(fg - \lambda f) < \rho(f)$. □

Codes from well-agreeing n-weights ρ and σ on R are constructed as follows (see [1]): there exists a basis $\mathcal{B} := \{f_i : i \in \mathbb{N}_0\} \cup \{g_j : j \in \mathbb{N}\}$ of R where $f_0 = 1$ and for all $i \in \mathbb{N}$, $f_i \in R, g_i \in \mathcal{U}_\rho$ are such that $\rho(f_i) = i$, $\sigma(g_i)$ is the ith element of $\sigma(\mathcal{U}_\rho^*)$ and $\sigma(f_i) = \min\{\sigma(f) : f \in R \text{ and } \rho(f) = i\}$. Consider the subspaces $R_\ell^m = \langle f_0, \ldots, f_\ell, g_1, \ldots, g_m\rangle$ of R and let $\varphi : R \to \mathbb{F}^n$ be a morphism of $\mathbb{F}$-algebras such that $\varphi(\cup_\ell R_\ell^t) = \mathbb{F}^n$ for t large enough. Then the obtained codes are $E_\ell^m := \varphi(R_\ell^m)$ and its dual $C_\ell^m := (E_\ell^m)^\perp$. As in the case of one single weight, the minimum distance of C_ℓ^m can be bounded in terms of the called *order bound*, which is obtained from the semigroup $H(R)$.

Finally we stress that, for practical applications of these codes, it is crucial again to characterize the algebras admitting well-agreeing weights. This is accomplished in the rest of this paper.

3. The semigroup structure

Let ρ and σ be two well-agreeing n-weights defined on an $\mathbb{F}$-algebra R. We generalize the definition of the set $H = H(R)$ stated in Section 2 to any $S \subseteq R$ by setting

$$H(S) := \{(\rho(f), \sigma(f)) : f \in S^*\} \subseteq \mathbb{N}_0^2,$$

where $S^* := S \setminus \{0\}$. We shall see that H is a semigroup. To that end, we need some preliminary results. For given $\mathbf{a} = (a_1, a_2)$ and $\mathbf{b} = (b_1, b_2)$ elements of $\mathbb{N}_0^2$, the *least upper bound* of $\mathbf{a}$ and $\mathbf{b}$ is defined as (cf. [13], [14])

$$\mathrm{lub}(\mathbf{a}, \mathbf{b}) := (\max\{a_1, b_1\}, \max\{a_2, b_2\}).$$

Lemma 3.1. *Let $f, g \in R^*$. Set $\mathbf{a} := (\rho(f), \sigma(f))$ and $\mathbf{b} := (\rho(g), \sigma(g))$. Then there exist $\lambda, \mu \in \{0, 1\}$ such that*

$$\mathrm{lub}(\mathbf{a}, \mathbf{b}) = (\rho(\lambda f + \mu g), \sigma(\lambda f + \mu g)).$$

In particular, if $f, g \in S \subseteq R$ and S is closed under addition, then $\mathrm{lub}(\mathbf{a}, \mathbf{b}) \in H(S)$.

Proof. If $\mathbf{a} = \mathbf{b}$ the result is obvious. Otherwise, we can assume $\rho(f) < \rho(g)$. If $\sigma(f) \leq \sigma(g)$, then $\mathrm{lub}(\mathbf{a}, \mathbf{b}) = \mathbf{b}$. On the contrary, if $\sigma(f) > \sigma(g)$ then

$$\max\{\rho(f), \rho(g)\} = \rho(f+g) \quad \text{and} \quad \max\{\sigma(f), \sigma(g)\} = \sigma(f+g)$$

and hence $\mathrm{lub}(\mathbf{a}, \mathbf{b}) = (\rho(f+g), \sigma(f+g))$. The second part is clear. □

Proposition 3.2. *If $S \subseteq R$ is closed under addition and multiplication, then $H(S)$ is closed under addition.*

Proof. Let $\mathbf{a} = (\rho(f), \sigma(f))$ and $\mathbf{b} = (\rho(g), \sigma(g))$ with $f, g \in S^*$. If $\mathbf{a} = \mathbf{0}$, the result is clear. If the integers $\rho(f), \sigma(f), \rho(g), \sigma(g)$ are all positive, that is, if $f, g \in \mathcal{M}_\rho \cap \mathcal{M}_\sigma$, then the result follows from property (N5) of n-weights. Thus assume $\rho(f) > 0$ and $\sigma(f) = 0$. There are three possibilities: (a) if $\rho(g) = 0$ and $\sigma(g) > 0$, then $\mathbf{a} + \mathbf{b} = \mathrm{lub}(\mathbf{a}, \mathbf{b}) \in H(S)$ according to Lemma 3.1; (b) if $\rho(g) > 0$ and $\sigma(g) = 0$, then $\mathbf{a} + \mathbf{b} = (\rho(fg), \sigma(fg)) \in H(S)$ by (N5); finally, (c) if $\rho(g) > 0$ and $\sigma(g) > 0$, then $\rho(fg) = \rho(f) + \rho(g)$ and $\sigma(fg) = \sigma(g)$ and hence $\mathbf{a} + \mathbf{b} = \mathrm{lub}(\mathbf{a}, \mathbf{c}) \in H(S)$, where $\mathbf{c} = (\rho(fg), \sigma(fg))$. □

Corollary 3.3. *Let R' be an $\mathbb{F}$-subalgebra of R. Then $H(R')$ is a semigroup.*

Next we consider the following sets associated to the semigroup $H = H(R)$:

$$H_x := \{(m, 0) \in H\}, \qquad H_y := \{(0, n) \in H\},$$

and their projections

$$\bar{H}_x := \{m : (m, 0) \in H\}, \quad \bar{H}_y := \{n : (0, n) \in H\}.$$

Clearly $\bar{H}_x$ and $\bar{H}_y$ are numerical semigroups of finite genus. For $n \in \mathbb{N}_0$, set

$$x_H(n) := \min\{m \in \mathbb{N}_0 : (m, n) \in H\} \quad \text{and} \quad y_H(n) := \min\{m \in \mathbb{N}_0 : (n, m) \in H\}.$$

Lemma 3.4. *If $y_H(n) > 0$, then $x_H(y_H(n)) = n > 0$. If $x_H(n) > 0$, then $y_H(x_H(n)) = n > 0$.*

Proof. Let $f \in R^*$ such that $\rho(f) = n$ and $\sigma(f) = y_H(n)$. By definition, $x_H(y_H(n)) \leq n$. If $\rho(g) < n$ and $\sigma(g) = y_H(n)$ for some $g \in R$, then there exists $\lambda \in \mathbb{F}$ such that $\sigma(f - \lambda g) < y_H(n)$. Since $\rho(f - \lambda g) = \rho(f)$, this is a contradiction. □

Corollary 3.5 (*cf. [10], [1, Cor. 4.8]*). *It holds that $n \in \mathrm{Gaps}(\bar{H}_x)$ if and only if $y_H(n) \in \mathrm{Gaps}(\bar{H}_y)$. In particular, the semigroups $\bar{H}_x$ and $\bar{H}_y$ have equal genus.*

We consider now the following subsets of H:

$$\tilde{\Gamma} = \tilde{\Gamma}(H) := \{(m, y_H(m)) : m \in \mathrm{Gaps}(\bar{H}_x)\} = \{(x_H(n), n) : n \in \mathrm{Gaps}(\bar{H}_y)\},$$
$$\Gamma = \Gamma(H) := \{(m, y_H(m)), (x_H(m), m) : m \in \mathbb{N}_0\} = \tilde{\Gamma} \cup H_x \cup H_y.$$

Note that $\tilde{\Gamma}$ is well-defined according to Lemma 3.4. The result below allows a nice description of the semigroup H.

Proposition 3.6 (*cf. [10,13]*). $H = \{\mathrm{lub}(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in \Gamma\}$.

Proof. According to Lemma 3.1, $\mathrm{lub}(\mathbf{a}, \mathbf{b}) \in H$ for all $\mathbf{a}, \mathbf{b} \in H$. Conversely, each $\mathbf{a} = (a_1, a_2) \in H$ can be written as $\mathbf{a} = \mathrm{lub}((a_1, y_H(a_1)), (x_H(a_2), a_2))$. □

For every $\mathbf{a} \in H$ take an element $\phi_{\mathbf{a}} \in R^*$ such that $(\rho(\phi_{\mathbf{a}}), \sigma(\phi_{\mathbf{a}})) = \mathbf{a}$, and set

$$\mathcal{B} := \{\phi_{\mathbf{a}} : \mathbf{a} \in \Gamma\}.$$

Proposition 3.7. *The set $\mathcal{B}$ is a basis of R as an $\mathbb{F}$-vector space.*

Proof. Since every two points $\mathbf{a} \neq \mathbf{b} \in \Gamma$ lie in different row and column, the set $\mathcal{B}$ is linearly independent, according to property (N2) of n-weights and Lemma 3.4. To see that $\mathcal{B}$ generate R take an element $f \in R^*$. Let us assume first that $\sigma(f) = 0$ and use induction on $\rho(f)$. If $\rho(f) = 0$ the result follows from the fact that $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$. If $\rho(f) = k > 0$, take $\phi_{\mathbf{a}} \in \Gamma$ with $\mathbf{a} = (k, 0)$. There exists $\lambda \in \mathbb{F}$ such that either $\lambda\phi_{\mathbf{a}} = f$ or $\rho(f - \lambda\phi_{\mathbf{a}}) < k$ and $\sigma(f - \lambda\phi_{\mathbf{a}}) = 0$. By induction hypothesis, all elements g with $\sigma(g) = 0$ and $\rho(g) < k$ are generated by $\mathcal{B}$ and hence f is generated by $\mathcal{B}$. According to Lemma 3.1 and Proposition 3.6, the general case $\sigma(f) > 0$ follows now by induction on $\sigma(f)$. □

For $(m, n) \in \mathbb{N}_0^2$ write $\Delta(m, n) := \{(m, \ell) : \ell < n\} \cup \{(\ell, n) : \ell < m\}$ and let $\mathrm{Gaps}(H)$ be the set of gaps of H.

Corollary 3.8 (*cf. [2]*). *We have*

$$\mathrm{Gaps}(H) = \bigcup_{\mathbf{a} \in \tilde{\Gamma}} \Delta(\mathbf{a}).$$

Proof. If $(m, n) \in \Delta(\mathbf{a})$ for some $\mathbf{a} \in \tilde{\Gamma}$, then $m < x_H(n) = a_1$ or $n < y_H(m) = a_2$; hence $(m, n) \notin H$. If $(m, n) \notin \Delta(\mathbf{a})$ for every $\mathbf{a} \in \tilde{\Gamma}$, then $n \geq y_H(m)$ and $m \geq x_H(n)$ and hence $(m, n) = \mathrm{lub}((m, y_H(m)), (x_H(n), n)) \in H$. □

Remark 3.9. In the case of Example 2.1, H is the Weierstrass semigroup at P and Q. A point $(m, n) \in \mathbb{N}_0^2$, is a gap of H if and only if $\ell(mP + nQ) = \ell((m-1)P + nQ)$ or $\ell(mP + nQ) = \ell(mP + (n-1)Q)$. Homma and Kim [9] noticed that AG codes associated to gaps (m, n) where both equalities above hold true, have quite good parameters; such gaps are called *pure*. Let $\mathrm{Gaps}_0(H)$ denotes the set of pure gaps of H. Then

$$\mathrm{Gaps}_0(H) = \bigcup_{\mathbf{a} \neq \mathbf{b} \in \tilde{\Gamma}} (\Delta(\mathbf{a}) \cap \Delta(\mathbf{b})).$$

Remark 3.10. For $m, n \in \mathbb{N}_0$, we can consider the subset of R

$$R(m, n) := \{f \in R : \rho(f) \leq m \text{ and } \sigma(f) \leq n\}.$$

In [1], subsets of this form were used to construct codes. Clearly $H(R(m,n)) = H(m,n) = \{\mathbf{a} = (a_1, a_2) \in H : a_1 \leq m \text{ and } a_2 \leq n\}$. Again in the case of Example 2.1, if $R = R(P, Q)$, then $H(m,n) = \mathcal{L}(mP + nQ)$. As a consequence of the Proposition 3.7, the set $\{\phi_{\mathbf{a}} : \mathbf{a} \in \Gamma \cap H(m,n)\}$ is a basis of $R(m,n)$.

4. The structure of the algebra R

By keeping the notation of the previous sections, let R be an $\mathbb{F}$-algebra and ρ and σ two well-agreeing n-weights on R. The semigroups $\bar{H}_x$ and $\bar{H}_y$ are finitely generated since they have finite genus. Write

$$\bar{H}_x = \langle m_1, \ldots, m_r \rangle, \quad \text{and} \quad \bar{H}_y = \langle n_1, \ldots, n_s \rangle$$

and define

$$\Gamma^+ = \Gamma^+(H) := \tilde{\Gamma} \cup \{(m_1, 0), \ldots, (m_r, 0), (0, n_1), \ldots, (0, n_s)\} \subseteq H.$$

Lemma 4.1. *Let $R' = \mathbb{F}[\{\phi_{\mathbf{a}} : \mathbf{a} \in \Gamma^+\}] \subseteq R$. Then $H(R') = H(R)$.*

Proof. Clearly $H(R') \subseteq H(R)$. To see the equality, according to Proposition 3.6 and Lemma 3.1, it suffices to show that $\Gamma \subseteq H(R')$. It is also clear that $\tilde{\Gamma} \subseteq H(R')$. Let $(m, 0) \in H_x$. There exist $\alpha_1, \ldots, \alpha_r \in \mathbb{N}_0$ such that $m = \sum \alpha_i m_i$. Thus the element

$$\phi = \prod \phi_{(m_i,0)}^{\alpha_i}$$

belongs to R'. Since $m_i > 0$ it follows that $\phi_{(m_i,0)} \in \mathcal{M}_\rho$. Thus

$$\rho(\phi) = \sum \alpha_i \rho(\phi_{(m_i,0)}) = \sum \alpha_i m_i = m \quad \text{and} \quad \sigma(\phi) \leq \sum \sigma(\phi_{(m_i,0)}) = 0.$$

Then $(m, 0) \in H(R')$. Analogously $H_y \subseteq H(R')$. □

Lemma 4.2. *Let R' be an $\mathbb{F}$-subalgebra of R. If $H(R') = H(R)$, then $R' = R$.*

Proof. Take $f \in R$ and let us see that $f \in R'$. We first consider the case $\sigma(f) = 0$. Let us write $\bar{H}_x = \{\ell_0 = 0 < \ell_1 < \ell_2 < \cdots\}$ and proceed by induction on $\rho(f)$. If $\rho(f) = 0$ then $f \in \mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$ and hence $f \in \mathbb{F} \subseteq R'$. By induction hypothesis assume that $f \in R'$ whenever $\rho(f) < \ell_k$, $k > 0$. If $\rho(f) = \ell_k$, take $f' \in R'$ such that $\rho(f') = \ell_k$ and $\sigma(f') = 0$. Thus, there exists $\lambda \in \mathbb{F}$ such that $\rho(f - \lambda f') < \ell_k$. Since $\sigma(f - \lambda f') \leq 0$, we get $f - \lambda f' \in R'$ and thus $f \in R'$.

Let us prove now the general case by induction on $\sigma(f)$. Assume the result true when $\sigma(f) < k + 1$. If $\sigma(f) = k$ take $f'' \in R'$ such that $\sigma(f'') = k$. Again there exists $\lambda \in \mathbb{F}$ such that $\sigma(f - \lambda f'') < k$; hence, by induction hypothesis, $f - \lambda f'' \in R'$ and so $f \in R'$. □

Theorem 4.3. *The $\mathbb{F}$-algebra R is finitely generated over $\mathbb{F}$, namely*

$$R = \mathbb{F}[\{\phi_{\mathbf{a}} : \mathbf{a} \in \Gamma^+\}].$$

Proof. It is a direct consequence of Lemmas 4.1 and 4.2. □

Proposition 4.4. *The $\mathbb{F}$-algebra R is an integral domain.*

Proof. By [1, Lemma 3.4] the set of zero divisors of R is contained in $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$; the proof now follows as ρ and σ are well-agreeing by hypothesis. □

As a consequence of the above theorem and proposition, R is isomorphic to an affine $\mathbb{F}$-algebra,

$$R \cong \mathbb{F}[X_1, \ldots, X_n]/\mathfrak{q},$$

where $\mathfrak{q}$ is a prime ideal. As an integral domain, R admits a field of quotients which we denote by $\mathbf{K}$.

Theorem 4.5. *The transcendence degree of $\mathbf{K}$ over $\mathbb{F}$ is one.*

In order to prove this theorem, we need some auxiliary results.

Lemma 4.6. *Let $f \in R^*$ and $I = (f)$ be the ideal generated by f. The sets $H_x \cap (\mathbb{N}_0^2 \setminus H(I))$ and $H_y \cap (\mathbb{N}_0^2 \setminus H(I))$ are both finite.*

Proof. We shall show that $H_y \cap (\mathbb{N}_0^2 \setminus H(I))$ is finite. If $f \in \mathbb{F}$ there is nothing to prove. Suppose that $f \notin \mathbb{F}$. Choose $g \in \mathcal{U}_\rho \setminus \mathbb{F}$. From Lemma 2.3 there exists $\lambda_1 \in \mathbb{F}$ such that $0 \leq \rho(fg_1) < \rho(f)$, where $g = g - \lambda_1$. If $\rho(fg_1) > 0$ we can again use Lemma 2.3 to find $g_2 \in R^*$ such that $0 \leq \rho(fg_2) < \rho(fg_1)$. Continuing in this way we can find $g \in R^*$ such that $\rho(fg) = 0$, and hence $\sigma(fg) > 0$. Let ℓ_σ be the largest gap of $\bar{H}_y$. Then, for all $m > \sigma(fg) + \ell_\sigma$ it holds that $\mathbf{a} = (0, m) \in H(I)$. Indeed, let a $\phi \in \mathbf{R}$ be a function such that $(\rho(\phi), \sigma(\phi)) = (0, m - \sigma(fg))$; then $fg\phi \in I$ and $(\rho(fg\phi), \sigma(fg\phi)) = \mathbf{a}$. The proof for H_x is analogous. □

Proposition 4.7. *Let $I \subseteq R$ be a proper ideal of R. Then, as a vector space over $\mathbb{F}$, $\dim_{\mathbb{F}}(R/I) \leq \#\{\mathbf{a} \in \Gamma : \mathbf{a} \notin H(I)\}$. In particular, this dimension is finite.*

Proof. Let $f \in I$, $f \neq 0$, and let $J = (f)$. For every $\mathbf{a} \in \Gamma$ take an element $\phi_\mathbf{a} \in \mathcal{B}$; that is, $(\rho(\phi_\mathbf{a}), \sigma(\phi_\mathbf{a})) = \mathbf{a}$. If $\mathbf{a} \in H(J)$ (resp. $\mathbf{a} \in H(I)$) take $\phi_\mathbf{a} \in J$ (resp. $\phi_\mathbf{a} \in I$). As we have seen in Proposition 3.7, the set $\mathcal{B}$ is a basis of R. Then

$$\dim(R/I) = \#\{\phi_\mathbf{a} + I : \mathbf{a} \in \Gamma\} \leq \#(\Gamma \setminus H(I)) \leq \#(\Gamma \setminus H(J)) < \infty$$

by Lemma 4.6. □

Proof of Theorem 4.5. According to Theorem 4.3, the $\mathbb{F}$-algebra R is finitely generated over $\mathbb{F}$. Thus the transcendence degree of $\mathbf{K}$ over $\mathbb{F}$ is equal to the Krull dimension of R; see Eisenbud [3, Thm. A, p. 223] or Matsumura [12, Ch. 5, Sect. 14]. Take $f \in R^*$ such that f is not invertible. Such an f exists: it is enough to take $f \in R \setminus \mathbb{F}$. Let $\mathfrak{p}$ be a minimal prime ideal containing f. Then $\text{height}(\mathfrak{p}) = 1$ by Krull's Hauptidealsatz; see [3, Thm. 10.2]. Since (see e.g. [3, Cor. 13.4] or [12, Thm. 14.H]),

$$\text{height}(\mathfrak{p}) + \dim(R/\mathfrak{p}) = \dim(R),$$

where 'dim' means Krull dimension, and $\dim(R/\mathfrak{p}) = 0$ according to Proposition 4.7, we get $\dim(R) = 1$. □

5. The main result

Let R be an $\mathbb{F}$-algebra equipped with two well-agreeing n-weights ρ and σ.

Lemma 5.1. *Let $f \in R^*$ and $I = (f)$ be the ideal generated by f. Then $H(I) \cup \{\mathbf{0}\}$ is a semigroup of finite genus.*

Proof. Let $\mathbf{a}$ and $\mathbf{b}$ be two different points in Γ and $\phi_\mathbf{a}, \phi_\mathbf{b} \in \mathcal{B}$. Note that $\phi_\mathbf{a} - \phi_\mathbf{b} \in I$ implies $\text{lub}(\mathbf{a}, \mathbf{b}) \in H(I)$ (as the points $\mathbf{a}, \mathbf{b}$ lie in different row and column). On the other hand, as we have seen in Proposition 3.6, $H = \{\text{lub}(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in \Gamma\}$. Since we can take $\phi_\mathbf{a} \in I$ except for finitely many $\mathbf{a} \in \Gamma$, we deduce that almost all elements in H belong to $H(I)$. □

Lemma 5.2. *Let $f \in R^*$. There exists $g \in \mathcal{M}_\rho$ such that $fg \in \mathcal{M}_\rho$.*

Proof. If $f \in \mathbb{F}^*$ then we are done. Assume that $f \notin \mathbb{F}^*$ and suppose that the result is false. Then $\rho(fg) = 0$ for all $g \in \mathcal{M}_\rho$. This implies that $f \in \mathcal{U}_\rho$, since otherwise $\rho(f) > \rho(1)$ and by (N3), $\rho(f^2) > \rho(f) > 0$. For any $g \in \mathcal{U}_\rho$ we have $\rho(fg) \leq \rho(f) + \rho(g) = 0$. Thus $I = (f) \subseteq \mathcal{U}_\rho$ and $H(I) \cup \{\mathbf{0}\}$ cannot be a semigroup of finite genus, in contradiction with Lemma 5.1. □

Define the map $\tilde{\rho} : R \to \mathbb{Z} \cup \{-\infty\}$ as follows: $\tilde{\rho}(0) := -\infty$ and for $f \neq 0$,

$$\tilde{\rho}(f) := \min\{\rho(fg) - \rho(g) : g \in \mathcal{M}_\rho\}.$$

In the following lemma we prove some relevant properties of $\tilde{\rho}$.

Lemma 5.3. (1) *$\tilde{\rho}$ is well-defined and $\tilde{\rho}(f) = \rho(fg) - \rho(g)$ for all $g \in \mathcal{M}_\rho$ such that $fg \in \mathcal{M}_\rho$;*

(2) *If* $f \in \mathcal{M}_\rho$, *then* $\tilde{\rho}(f) = \rho(f) > 0$; *if* $f \in \mathcal{U}_\rho$, *then* $\tilde{\rho}(f) \leq 0$;
(3) $\tilde{\rho}(f) = 0$ *for all* $f \in \mathbb{F}^*$;
(4) $\tilde{\rho}(fg) = \tilde{\rho}(f) + \tilde{\rho}(g)$;
(5) $\tilde{\rho}(f+g) \leq \max\{\tilde{\rho}(f), \tilde{\rho}(g)\}$.

Proof. (1) Let $g_1, g_2 \in \mathcal{M}_\rho$ such that $fg_1 \in \mathcal{M}_\rho$. Then $\rho(fg_1) + \rho(g_2) = \rho(fg_1g_2) \leq \rho(fg_2) + \rho(g_1)$, hence $\rho(fg_1) - \rho(g_1) \leq \rho(fg_2) - \rho(g_2)$, with equality when $fg_2 \in \mathcal{M}_\rho$. (2) and (3) are immediate. (4) By Lemma 5.2, there exists $h \in \mathcal{M}_\rho$ such that $fgh, gh \in \mathcal{M}_\rho$. Then $\tilde{\rho}(fg) = (\rho(fgh) - \rho(gh)) + (\rho(gh) - \rho(h)) = \tilde{\rho}(f) + \tilde{\rho}(g)$. (5) Let $h \in \mathcal{M}_\rho$ such that $fh, gh \in \mathcal{M}_\rho$. Then $\tilde{\rho}(f+g) \leq \rho((f+g)h) - \rho(h) \leq \max\{\tilde{\rho}(f), \tilde{\rho}(g)\}$. □

Define now the map $v_\rho : \mathbf{K} \to \mathbb{Z} \cup \{\infty\}$ by:

$$v_\rho(f/g) := \begin{cases} \infty & \text{if } f = 0, \\ \tilde{\rho}(g) - \tilde{\rho}(f) & \text{if } f \neq 0. \end{cases}$$

Properties in Lemma 5.3 imply the following.

Proposition 5.4. *The map* v_ρ *is well-defined and gives a discrete valuation of* $\mathbf{K}$ *over* $\mathbb{F}$.

Analogously we can define the valuation v_σ associated to the n-weight σ. Denote by $\mathbb{P}(\mathbf{K})$ the set of places of $\mathbf{K}$ over $\mathbb{F}$. For a place $S \in \mathbb{P}(\mathbf{K})$, let v_S and $\mathcal{O}_S$ be the corresponding valuation and valuation ring in $\mathbf{K}$. Set

$$\mathcal{S}(R) := \{S \in \mathbb{P}(\mathbf{K}) : R \subseteq \mathcal{O}_S\}.$$

Proposition 5.5 (*cf. [11, p. 2009]*). *Let* P *and* Q *be the places of* $\mathbf{K}$ *corresponding to* v_ρ *and* v_σ (*see Proposition* 5.4). *Then*

$$\mathcal{S}(R) = \mathbb{P}(\mathbf{K}) \setminus \{P, Q\}.$$

Proof. If $R \subseteq \mathcal{O}_P$ then $\mathcal{U}_\rho = R$ hence $\mathcal{M}_\rho = \emptyset$ and the semigroup $H(R)$ cannot have a finite genus. Thus $P, Q \notin \mathcal{S}(R)$. Conversely, if $\mathcal{S}(R) \cup \{P, Q\} \neq \mathbb{P}(\mathbf{K})$, we can apply to $\mathcal{S}(R) \cup \{P, Q\}$ the Strong Approximation Theorem (see e.g. Stichtenoth [16, I.6.4]) to conclude that there exists a infinite sequence $(h_1, h_2, \ldots)$ of functions in $\mathbf{K}$ such that $v_\rho(h_i) = v_\sigma(h_i) = i$ and $v_S(h_i) \geq 0$ for each $S \in \mathcal{S}(R)$. In particular, $h_i \in \cap_{S \in \mathcal{S}(R)} \mathcal{O}_S$ and this ring is precisely $\bar{R}$, the integral closure of R in $\mathbf{K}$ (see e.g. [16, III.2.6]). The sequence $(h_1, h_2, \ldots)$ is $\mathbb{F}$-linearly independent and contained in the $\mathbb{F}$-vector space

$$W := \{x \in \bar{R} : v_\rho(x) > 0 \text{ and } v_\sigma(x) > 0\}.$$

As the n-orders ρ and σ are well-agreeing, we have $W \cap R \subseteq \mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$, and thus $W \cap R = \{0\}$. Then $\dim_{\mathbb{F}}(W) = \dim_{\mathbb{F}}(W/(W \cap R)) = \dim_{\mathbb{F}}(W + R)/R \leq \dim_{\mathbb{F}}(\bar{R}/R)$. But, according to the Finiteness of Integral Closure Theorem (see e.g. [3, Cor. 13.13] or Zariski–Samuel [18, Ch. V, Thm. 9]), this last dimension is finite and we get a contradiction. □

Thus, we have proved the following.

Theorem 5.6. *Let* R *be an* $\mathbb{F}$*-algebra admitting two well-agreeing* n*-weights* ρ *and* σ. *Then*

(1) R *is an integral domain and its quotient field* $\mathbf{K}$ *is an algebraic function field of one variable over* $\mathbb{F}$;
(2) *There exist two places* $P, Q \in \mathbb{P}(\mathbf{K})$ *such that* ρ *and* σ *are derived from the valuations associated to* P *and* Q *by the procedure stated in Example* 2.1; *and*
(3) $\bar{R} = \cap_{S \in \mathbb{P}(\mathbf{K}) \setminus \{P, Q\}} \mathcal{O}_S$.

Remark 5.7. Let R be an integral domain $\mathbb{F}$-algebra having Krull dimension 1, and let $\mathbf{K}$ be its field of quotients. Let $P, Q \in \mathbb{P}(\mathbf{K})$. By using the procedure of Example 2.1, the valuations at P and Q define two n-weights, ρ and σ, over R. Let us note that condition (3) in Theorem 5.6 can be stated also as $\mathcal{S}(R) = \mathbb{P}(\mathbf{K}) \setminus \{P, Q\}$. In this case it holds that $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = \mathbb{F}$. In fact, if $f \in R$ is such that $v_P(f) \geq 0$ and $v_Q(f) \geq 0$, then $f \in \cap_{S \in \mathbb{P}(K)} \mathcal{O}_S = \mathbb{F}$ by [16, III.2.6]. Thus ρ and σ agree well if and only if $\#(\mathbb{N}_0^2 \setminus H(R))$ is finite. This observation leads to the following question: Does condition (3) imply that $\#(\mathbb{N}_0^2 \setminus H(R)) < \infty$?

Problem. Characterize the $\mathbb{F}$-algebras R, satisfying condition (3) of Theorem 5.6 and such that $\mathbb{N}_0^2 \setminus H(R)$ is finite.

Remark 5.8. Note that in the above problem, the normalization of n-weights in again crucial. To see this, take the example given in Remark 2.2. Let $\mathbf{K} := \mathbb{F}_2(x)$ be the rational function field of characteristic two. Let S be the ring of all functions of $\mathbf{K}$ which are regular away from two places P, Q, and let $R := \{f^2 : f \in S\}$. The integral closure of R in $\mathbf{K}$ is S (see e.g. [16]), so condition (3) of Theorem 5.6 is satisfied with or without normalization. But, as noted in Remark 2.2, the cardinality $\mathbb{N}_0^2 \setminus H(R)$ is finite in one case and infinite in the other.

Acknowledgments

The authors thank the reviewer for the interesting suggestions and the example of Remark 2.2 and the editor for her quick and efficient management of this paper. The authors were supported respectively by the "Junta de Castilla y León", España, under Grant VA020-02, and CNPq-Brazil (306676/03-6) and PRONEX (66.2408/96-9).

References

[1] C. Carvalho, C. Munuera, E. Silva, F. Torres, Near orders and codes, IEEE Trans. Inform. Theory 53 (5) (2007) 1919–1924.
[2] C. Carvalho, F. Torres, On Goppa codes and Weierstrass gaps at several points, Des. Codes Cryptogr. 35 (2) (2005) 211–225.
[3] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer-Verlag, New York, 1995.
[4] G.L. Feng, T.R.N. Rao, Improved geometric Goppa codes part I, basic theory, IEEE Trans. Inform. Theory 41 (6) (1995) 1678–1693.
[5] O. Geil, R. Pellikaan, On the structure of order domains, Finite Fields Appl. 8 (2002) 369–396.
[6] V.D. Goppa, Codes associated with divisors, Probl. Inf. Transm. 13 (1977) 22–26.
[7] V.D. Goppa, Geometry and Codes, in: Mathematics and its Applications, vol. 24, Kluwer, Dordrecht, 1991.
[8] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: V. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, 1998, pp. 871–961.
[9] M. Homma, S.J. Kim, Goppa codes with Weierstrass pairs, J. Pure Appl. Algebra 162 (2001) 273–290.
[10] S.J. Kim, On the index of the Weierstrass semigroup of a pair of points on a curve, Arch. Math. 62 (1994) 73–82.
[11] R. Matsumoto, Miura's generalization of one-point AG codes is equivalent to Høholdt, van Lint and Pellikaan's, IEICE Trans. Fundam. E82-A (10) (1999) 2007–2010.
[12] H. Matsumura, Commutative Algebra, W.A. Benjamin Co., New York, 1970.
[13] G. Matthews, The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve, in: A. Poli, H. Stichtenoth (Eds.), Fq7, Springer, Berlin, 2004, pp. 12–24.
[14] G. Matthews, Some computational tools for estimating the parameters of algebraic geometry codes, Contemp. Math. 381 (2005) 19–26.
[15] R. Pellikaan, On the existence of order functions, J. Stat. Plan. Inference 94 (2001) 287–301.
[16] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, New York, Berlin, 1993.
[17] M.A. Tsfasman, S.G. Vladut, T. Zink, Modular curves, Shimura curves and Goppa codes, better than Varshamov–Gilbert bound, Math. Nachr. 109 (1982) 21–28.
[18] O. Zariski, P. Samuel, Commutative Algebra, vol. I, Van Nostrand, Princeton, 1958.